Список використаних джерел:

1. Іншин М.І. Загальнотеоретична характеристика дистанційної зайнятості працівників в Україні. Право і суспільство. 2015. №5.2. С. 123-128.
2. Лісогор Л.С., Руденко Н.В., Чувардинський В.О. Конкурентоспроможність робочої сили: проблеми формування та реалізації в умовах інноваційних змін на ринку праці. Економіка і організація управління. 2018. Вип. 3. С. 24-36.
3. Петюх В.М., Шеіна В.О., Шепель А.Ю. Загальні компетенції та якості, необхідні молоді для створення власного бізнесу. Молодий вчений. 2016. №5. С. 126-130.
4. Піщуліна О. Цифрова економіка: тренди, ризики та соціальні детермінанти. К.: Центр Разумкова, Видавництво «Заповіт», 2020. 274 с.
5. Червінська Л.П. Проблематика змісту праці в Україні. Соціально-трудові відносини: теорія та практика. 2017. №1. С. 117-124.

УДК 658.5

Савеленко Г. В., к.т.н., доц.,
Шевчук К. А.
Центральноукраїнський національний технічний університет,
м. Кропивницький

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА В СУЧАСНИХ УМОВАХ

Інформатизація сьогодення поширилась на всі сфери життя людини. Зорієнтуватись в сучасному інформаційному потоці без допомоги комп'ютерної техніки та програмного забезпечення досить складно або майже не можливо. Найшвидше розвиваються технології, по'вязані з глобальною комп'ютерною мережею Інтернет. Це призвело до появи і поширення таких категорій, як електронний бізнес, електронний уряд та ін. [1].

Зі зростанням інформатизації стає більш жорсткою конкуренція, яка свої активні дії все частіше переводить в інформаційний простір. До загроз інформаційної безпеки підприємства можна віднести дії або процеси щодо інформаційних ресурсів даного підприємства, які можуть їх спотворити, пошкодити або надати до них доступу третім особам. Втрата стратегічно важливої інформації може призвести до штрафів, втрати ділової репутації або й втрати контролю над управлінням підприємством.

Враховуючи джерела виникнення загроз інформаційної безпеки їх прийнято розділяти на зовнішні (конкуренти, зловмисники, соціальна інженерія, промислове шпигунство) та внутрішні (необережні дії або навмисні дії персоналу при розголошенні важливої інформації).

Зовнішні загрози найчастіше виникають у результаті наступних дій [2]:

– несанкціонованого копіюванні секретних документів, або викрадення файлів з ними;
– викрадення носіїв інформації;
– викрадення інформації у процесі її передавання по мережі Інтернет;
– пошкодження програмних і апаратних засобів на підприємстві;

– розповсюдження інформації до фірм-конкурентів, або інших зацікавлених сторін;

– викрадення інформації за допомогою інсайдерів.

До причин внутрішніх загроз можна віднести:

– причини психологічного характеру у зв'язку з впровадженням нових інформаційних технологій;

– незадоволенням рівня матеріальних та нематеріальних стимулів;

– відсутність практики впровадження на підприємстві договору про нерозголошення конфіденційної інформації.

На сучасному підприємстві практично кожен працівник може стати носієм цінних, конфіденційних відомостей, які становлять інтерес для конкурентів та інших зацікавлених осіб. Також існує загроза нанесення шкоди підприємству внаслідок недбалості, безвідповідальності, банального незнання правил роботи з конфіденційною інформацією та її захисту.

Для зменшення впливу вище окреслених загроз та підвищення інформаційної безпеки на підприємстві пропонуємо дотримуватись наступних правил:

– підвищення кваліфікації персоналу в області нових інформаційних технологій;

– використання криптографічних методів захисту для секретних даних та електронного листування;

– перехід на підприємстві до електронного документообігу;

– конфіденційні дані потрібно розміщувати на окремих сертифікованих серверах або хмарних сервісах.

Сьогодні в умовах ринкових відносин підприємства є самостійними у виборі своєї економічної політики, виборі постачальників, організації виробництва та збуту продукції, впровадженні режиму комерційної таємниці на підприємстві та типу договорів про нерозголошення. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити дієву систему управління інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства неможливо забезпечити стабільну роботу його бізнес-процесів.

Список використаних джерел:

1. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. – 2011. – № 21. – С. 92-95.

2. Качан О.І. Інформаційна безпека підприємства в умовах глобалізації / О.І. Качан // Розвиток малого та середнього бізнесу в умовах глобалізації світової економіки : матеріали виступів Всеукраїнського економічного форуму з міжнародною участю (в онлайн форматі) (27 квітня 2017 року). – Житомир : ЖДТУ, 2017. – 392 с. (Електронне видання)